U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE

HEARING CHARTER

The Future of Computer Science Research in the U.S.

Thursday, May 12, 2005
10:00 a.m. - Noon
2318 Rayburn House Office Building

1. Purpose

On Thursday, May 12, 2005, the House Science Committee will hold a hearing to examine the state of computer science research in the United States and the evolution of federal support for this field. Specifically, the hearing will examine the controversy surrounding the apparent shift away from basic research in overall federal support for computer science and the impact of the shift on federal agencies, academia and industry.

2. Witnesses

Dr. John H. Marburger III is Director of the Office of Science and Technology Policy (OSTP), the White House science office. Prior to joining OSTP, Dr. Marburger served as President of the State University of New York at Stony Brook and as Director of the Brookhaven National Laboratory.

Dr. Anthony J. Tether is the Director of the Defense Advanced Research Projects Agency (DARPA). Prior to his appointment as Director of DARPA in 2001, Dr. Tether served as Chief Executive Officer of The Sequoia Group and of Dynamics Technology Inc.

Dr. Wm. A. Wulf is president of the National Academy of Engineering. He is on leave from the University of Virginia, Charlottesville, where he is a University Professor and AT&T Professor of Engineering and Applied Sciences. His research focuses on computer architecture and computer security. He served as Assistant Director for Computer and Information Science and Engineering at the National Science Foundation from 1988 to 1990.

Dr. Tom Leighton is Chief Scientist and co-founder of Akamai Technologies. His expertise is in algorithms for network applications, which he used to develop a solution to freeing up internet congestion. In addition to his position at Akamai, he is a Professor of Applied Mathematics at the Massachusetts Institute of Technology. He is currently a member of the President's Information Technology Advisory Committee (PITAC) and served as chairman of the committee's subcommittee on cybersecurity.

3. Brief Overview

- Federal support for information technology research has been a key to the development of the information technology industry. The 2003 National Academy of Sciences report *Innovation in Information Technology* lists 19 areas in which federally sponsored fundamental research underpinned the innovations that eventually became multibillion-dollar information technology industries. Examples include the Internet and the World Wide Web, parallel and relational databases, data mining, and speech recognition.

- Academic computer science research has direct relevance to the information technology industry. University research in computer science is funded by a number of agencies within the federal government, but the largest contributors are the Defense Advanced Research Projects Agency (DARPA) and the National Science Foundation (NSF), which together accounted for about 85 percent of the roughly $1.1 billion of federal funding for research performed at universities and colleges in mathematics and computer sciences in fiscal year 2004 (FY04).

- Recently, many computer science researchers have become concerned about an apparent trend at DARPA toward reducing the percentage of DARPA's computer science research portfolio dedicated to long-term fundamental research. DARPA's withdrawal may have contributed to increased proposal pressures on NSF, which has experienced a doubling of applications for funding relating to computer science over the last four years, causing application approval rates to plummet.

- DARPA and NSF programs are complementary, but have many significant differences. While both agencies award grants competitively, DARPA has its program managers select the awardees, while NSF uses a peer-review process. Peer review allows a wider range of views to be considered, but also tends to be more conservative. DARPA awards also tend to be targeted to a more specific end-product even though that product may be many years away. The general view in the computer science field is that both agencies need to support fundamental research to allow for a balanced national portfolio. A sense of the relative strengths of the two agencies can be seen in the development of the Internet. DARPA-sponsored research led to the initial forerunner of the Internet, known as ARPANET. NSF funding led to the expansion of networks (initially for university use) and to the development of the World Wide Web.

- In March 2005, the President's Information Technology Advisory Committee (PITAC) released a report entitled *Cybersecurity: A Crisis of Prioritization*. In it, the committee describes the importance of federally supported research in cybersecurity and recommends additional federal investment at several agencies (including NSF and DARPA) to develop the next generation of cybersecurity technologies and increase the size of the cybersecurity research community. The PITAC report also recommends strengthening cybersecurity technology transfer efforts and improving interagency coordination of cybersecurity research programs.

- The Science Committee has been a leader in pushing for increased research in cybersecurity through, for example, passage in 2002 of the *Cyber Security Research and Development Act*

(P.L. 107-305), which authorized $903 million over five years for cybersecurity research and fellowship programs at NSF and at the National Institute of Standards and Technology. In FY 05, NSF cybersecurity programs are funded at about $82 million, $46 million below the level authorized in the Act.

4. Overarching Questions

- What effects are shifts in federal support for computer science—e.g. shifts in the balance between short- and long-term research, shifts in the roles of different agencies—having on academic and industrial computer science research and development? What impacts will these changes have on the future of the U.S. information technology industry and on innovation in this field?

- Are the federal government's current priorities related to computer science research appropriate? If not, how should they be changed?

- What should the federal government be doing to implement the recommendations of the recent President's Information Technology Advisory Committee (PITAC) report on cybersecurity?

5. Background

Federal Support for Information Technology Research

Many of the technologies that enabled electronic commerce to take off in the 1990s are based on research initially conducted at universities and funded by DARPA and NSF. The 2003 National Academy of Sciences (NAS) report *Innovation in Information Technology* lists 19 areas in which federally sponsored fundamental research underpinned the innovations that eventually became multibillion-dollar information technology industries.[1] Examples relating to e-commerce include web browsers, search engines, cryptography methods that allow secure credit card transactions, databases to manage information and transactions, and the protocols and hardware underlying the Internet itself. Often, the unanticipated results of such research are as important as the anticipated results. For example, the early research that led to e-mail and instant messaging technologies was originally done in the 1960s as part of a project examining how to share expensive computing resources among multiple simultaneous and interacting users.

These innovations have helped create an information technology sector that is credited for nearly 30 percent of real growth in the U.S. gross domestic product from 1994 to 2000 and that currently accounts for 29 percent of all U.S. exports.[2] The military also depends heavily on the information technology sector's commercial-off-the-shelf products to meet its critical information technology needs.

Since the pace of change in information technology products is so rapid, companies' main competitive advantage often comes from being first to market with a particular product or

[1] Computer Science and Telecommunications Board, National Academies, *Innovation in Information Technology*, National Academy Press (2003), pages 6-7.
[2] Data from the Information Technology Industry Council, http://www.itic.org/sections/Economy.html.

feature. If the U.S. research community isn't producing the ideas, or if the ideas are classified, it is less likely that U.S. companies will be the first to benefit from the research results.

Academic research also contributes to the training of the information technology workforce. Research grants support graduate students, and undergraduate and graduate computer science and engineering programs at universities produce the software developers and testers, hardware designers, and other personnel that power the computing and communications industries and the industries that depend on information technologies. (For example, automotive and manufacturing companies rely on modeling and simulation for product development and production management, and the financial services sectors utilize information technology for modeling markets and securing financial transactions.)

Agencies That Support Academic Computer Science Research

University research in computer science is funded by a number of agencies within the federal government but the largest contributors are DARPA and NSF, which together accounted for about 85 percent of the roughly $1.1 billion of federal funding for research performed at universities and colleges in mathematics and computer sciences in FY04. Other agencies that contribute in this area include the National Institutes of Health, the National Aeronautics and Space Administration, the Department of Energy, and the research agencies of the Armed Forces. Coordination among the agencies primarily occurs through working groups organized under the multi-agency National Information Technology Research and Development Program (NITRD), which operates under the auspices of the White House Office of Science and Technology Policy.

Defense Advanced Research Projects Agency

DARPA's mission is to ensure that the U.S. military remains, over the long-run, at the cutting edge of technology. DARPA conducts its mission by sponsoring revolutionary, high-payoff research that bridges the gap between fundamental discoveries and their military use. (The research it sponsors tends to be more revolutionary and more targeted than the research funded by NSF.) DARPA does not conduct any research itself; it sponsors research in academia and industry. DARPA's programs are organized around strategic thrusts in areas of importance to national security, and projects are sought out and selected by program managers. These program managers usually come to DARPA on leave from technical positions in the private sector, other government agencies, or academia and usually stay at DARPA for about four to six years. DARPA program managers are encouraged to pursue high-risk technical ideas and have the authority to quickly make decisions about starting, continuing, or stopping research projects.

DARPA played a key role in the birth and maturation of computer science as a field and the development of many of the important subspecialties. As described by the NAS report, DARPA helped start many of today's university computer science programs by funding large-scale university centers of excellence early in the history of the computer science field.

DARPA supported research that produced advances in areas as diverse as computer graphics, artificial intelligence, networking, and computer architecture.[3] A recent Defense Science Board report also describes the unique role DARPA has played. DARPA program managers have encouraged simultaneous yet competing work by industrial and university researchers on the technological barriers to new computing capabilities and has also funded university researchers to produce convincing prototypes of revolutionary concepts.[4]

However, in the past five years, the computer science research community in both academia and industry has raised concerns that DARPA has been narrowing its focus. The community believes DARPA has been moving away from investing in longer-term basic research in favor of increased funding for development of specific technologies for the armed forces' more immediate defensive and offensive needs. They believe that this change in focus is evident in a number of ways—a reduction of funding for university research in computer science, an increase in classification of research programs and restriction on participation of non-citizens, and reviews of whether to continue funding individual research projects at 12- to 18-month intervals, which is short for fundamental research.[5,6] These concerns recently received public airing in an article on the front page of the business section of the *New York Times* (Attachment A) and an editorial in Science magazine (Attachment B).

The way DARPA categorizes its research makes it difficult to get a complete picture of the trends in its computer science research. DARPA's budget requests, relevant appropriations language, and project portfolio management are organized in a constantly changing array of "program elements" rather than by field. However, in response to a Congressional request for historical data on DARPA funding for computer science and the amount of that funding given to universities, DARPA reviewed individual projects from the recent past to determine which could be classified as computer science research. The data was provided for FY01 through FY04 (Table 1) and showed that while overall computer science funding grew slightly (from $546 million in FY01 to $583 million in FY04), funding awarded to universities for computer science research declined each year in that period, going from $214 million in FY01 to $123 million in FY04 (a drop of 43 percent).

Table 1: DARPA funding for computer science research, overall and at universities (dollars in millions).

	FY01	**FY02**	**FY03**	**FY04**
Total DARPA Funding	1,884	2,260	2,655	2,815
Total DARPA Computer Science Funding	546	571	613	583
Amount of Computer Science Funding Awarded to Universities	214	207	173	123

Source: DARPA communication to Senate Armed Services Committee Staff
Note: Data was only provided for these four years.

[3] Computer Science and Telecommunications Board, National Academies, *Innovation in Information Technology*, National Academy Press (2003), pages 23-25.
[4] Report of the Defense Science Board Task Force on High Performance Microchip Supply, February 2005, page 87.
[5] "An Endless Frontier Postponed," by Edward D. Lazowska and David A. Patterson, SCIENCE Magazine, Volume 308, May 6, 2005, page 757.
[6] Report of the Defense Science Board Task Force on High Performance Microchip Supply, February 2005, page 88.

Another source of information on the changing role of DARPA in supporting university computer science research is data gathered by the Computing Research Association. These data show that at leading university computer science departments, both the dollar amount of funding received from DARPA, and the percent of their funding from DARPA dropped sharply between FY99 and FY04. The percentage of their funding from DARPA in FY04 was roughly half of what it was in FY99.

DARPA has cited several factors that have contributed to this decline in its funding for university computer science research. First, much more DARPA computing research is classified, and universities generally do not perform classified research. The impact of increased classification has been particularly noticeable in the area of information assurance (also known as cybersecurity) for which the unclassified budget dropped by 50 percent between FY01 and FY04, leading to a drop in university funding from $20 million to $4 million. Second is the congressional termination[7] in FY04 of DARPA's program on asymmetric threats, which included approximately $11 million in university funding.

The third and perhaps most critical explanation for why DARPA's funding for university computer science research has declined is that work in many ongoing programs has progressed from the research phase to the product development and construction phase. For example, DARPA notes that work on high-performance computing has moved from research on how to design new computers to product development, leading funding to shift from universities to industry. Similarly, work in intelligent software has gone beyond the fundamental research stage, leading DARPA funding in that area for universities to decline from about $28 million in FY01 to about $8 million in FY04. But computer scientists argue that, while work has progressed in these programs, there is basic research to be pursued in other, new areas.

Finally, DARPA may be feeling increasing pressure from the Department of Defense and the individual armed services to more quickly develop new technologies that can be deployed to meet current and near-term needs. DARPA has always played a critical role in the development of technologies for the armed forces. Examples of current DARPA programs with important short-term impacts include the Marine Airborne Retransmission System program, which helps extend the range of tactical radios and is expected to be deployed with the Marine Corps in Iraq very soon, and work on operating systems for unmanned combat air vehicles.

DARPA has always carried out a mix of nearer- and longer-term work and the question is whether the current balance is appropriate. Academic and some industry researchers fear that the balance is now shifting too much in the direction of nearer-term work, which will deprive the U.S. industry (and military) of ideas that could be helpful in the future. For example, research is needed on how to integrate nanotechnology and biotechnology with information technology systems.

[7] DARPA's work on asymmetric threats was terminated as part of congressional elimination of DARPA's larger Terrorism Information Awareness program (also known as Total Information Awareness) in FY04 due to congressional concerns about the appropriateness of the overall program goals.

National Science Foundation

Like DARPA, NSF performs no research itself. At NSF, projects are selected for funding through a competitive, peer review process, in which NSF brings together panels of experts in a given field to review proposals anonymously. Researchers can send project proposals to NSF either in response to agency-issued requests for proposals in specific areas or as unsolicited proposals.

Computer science research at NSF is conducted almost entirely in the Computer and Information Sciences and Engineering Directorate (CISE), although the directorate funding is not entirely devoted to computer science research. Relevant CISE activities include support for investigator-initiated research in all areas of computer and information science and engineering; development and maintenance of cutting-edge national computing and information infrastructure for research and education in many fields; and support for the education and training of the next generation of computer scientists and engineers.

In the five years between FY00 and FY04, the number of proposals received at CISE annually has more than doubled (Table 2). While funding has also increased, it has not kept pace with increasing proposal pressure and the rising costs of doing research. As a result, the success rate for proposals dropped to 16 percent, which is the lowest of any NSF directorate. During the same time period, the percentage of federal funding for research performed at universities and colleges in mathematics and computer sciences that was provided by NSF grew from 55 percent to 65 percent.[8]

Table 2: Proposal Pressure within the NSF Computer and Information Sciences and Engineering directorate

	FY00	**FY01**	**FY02**	**FY03**	**FY04**
NSF Total Funding ($ in millions)	$3948	$4454	$4789	$5308	$5652
CISE Total Funding ($ in millions)	$389	$478	$515	$589	$605
Number of Proposals to CISE	3,022	3,866	4,540	5,612	6,496
Number of Grants Awarded by CISE	931	923	1,093	1,231	1,064
CISE Success Rate	31%	24%	24%	22%	16%
Overall NSF Success Rate	33%	31%	30%	27%	24%

Note 1: Statistics are for "competitively reviewed" proposals and awards (i.e. proposal actions for research, education, and training grants processed through NSF's merit review system each year). Funding for second-year and later increments for continuing grants are not included.

Note 2: Over this same period, the average grant size in CISE increased from $153,840 in FY00 to $175,692 in FY04, and the number of senior personnel supported doubled, rising from 1,985 to 3,908.

Source: *Report to the National Science Board on the National Science Foundation's Merit Review Process: Fiscal Year 2004*, NSB-05-12, March 2005, pages 29 and 31.

A number of factors have contributed to this rise in proposal pressure and the drop in success rate. One is the growing number of computer science faculty looking to the federal government for research support. From the 1999-2000 academic year to the 2003-2004 academic year, the

[8] *Federal Funds for Research and Development: Fiscal Years 2002, 2003, and 2004*; *Federal Funds for Research and Development: Fiscal Years 2001, 2002, and 2003*; and *Federal Funds for Research and Development: Fiscal Years 2000, 2001, and 2002*. All compiled by the NSF Division of Science Resources Statistics.

number of faculty in the top 24 U.S. computer science departments increased by 27 percent (nearly 300 new faculty), and similar growth patterns were seen in the total number of faculty at all computer science departments.[9] Another factor is the growth of interest in the types of computer science-related programs funded by CISE. As researchers from other disciplines have discovered the value of information technology in tackling outstanding questions in their fields, scientists in physics, oceanography, biology, and many other areas have begun to seek funding from CISE. Finally, while the number of proposals was rising, CISE was also making a concerted effort to increase grant size in order to enhance researchers' productivity and improve opportunities for training students. While this strategy was consistent with recommendations made by PITAC and overall NSF goals, it also limited CISE's ability to increase the number of grants awarded.

Given the multitude of factors that have contributed to the increase in proposals submitted to CISE, it is difficult to determine how much of this change is due to researchers shifting their focus to NSF from DARPA because of the increasing difficulty of getting DARPA grants.

How DARPA and NSF Complement Each Other

Both DARPA and NSF have played a critical role in the development of computer science. NSF programs are generally driven by researchers' proposals and peer review while DARPA's investments are generally driven by the priorities set out by program managers who try to push the research envelope to meet particular military and national needs. NSF support is essential to the ongoing research and education work of a broad computer science community; DARPA work is essential to pulling that community into specific, newer areas. Both agencies have funded work that has led to technological leaps in information technology.

The Science Committee has been reviewing the relationship between the two agencies for some time. For example, on May 14, 2003, the Science Committee held a hearing to examine federal cybersecurity R&D activities. At the hearing, Dr. Tether, the director of DARPA, in response to a question about whether the federal government was giving sufficient priority to the needs of cybersecurity, answered that DARPA is "more idea limited right now than we are funding limited," and indicated that DARPA relied on NSF to supply ideas. That appeared to be a shift away from DARPA's historic role, in which it funded fundamental research to foster new ideas as well as working to bring ideas to the development stage. Also many computer scientists expressed surprise at the DARPA comment, arguing that numerous ideas for research were going begging for money.

PITAC Report—Cybersecurity: A Crisis of Prioritization

On March 18, 2005, the President's Information Technology Advisory Committee (PITAC) released their report *Cybersecurity: A Crisis of Prioritization*. (The Executive Summary of the report is Attachment C.) In it, the committee argues for increased federal funding for cybersecurity research and emphasizes the important and complementary roles multiple agencies play in ensuring that the next generation of cybersecurity technologies will be developed and implemented.

[9] Annual Taulbee Surveys from the Computing Research Association. Available on line at http://www.cra.org/statistics/.

Specifically, the report presents four findings and recommendations. The first recommendation is that Congress and the Administration should substantially increase funding for fundamental research in civilian cybersecurity at a number of agencies, especially NSF, DARPA, and the Department of Homeland Security (DHS). In particular, the report recommends that funding for cybersecurity research at NSF be increased by $90 million annually.

The second recommendation from the committee is that the federal government increase its support for recruitment and retention of cybersecurity researchers and students at research universities, with a goal of at least doubling the size of the civilian cyber security fundamental research community by the end of the decade. In particular, the report recommends increased, stable funding for research, recruitment of people from other fields into cybersecurity, and increased emphasis on the importance of unclassified cybersecurity research.

The third recommendation from the committee is that, because current cyber security technology transfer efforts are not adequate to move the results of federal research investments into civilian sector best practices and products, the federal government should strengthen its cyber security technology transfer partnership with the private sector. Examples of what the federal government could do include: placing greater emphasis on the development of metrics, models, datasets, and testbeds so that new products and best practices could be evaluated; and encouraging Federally supported graduate students and postdoctoral researchers to gain experience in industry as researchers, interns, or consultants.

The final recommendation from the committee is that the federal government should improve coordination and oversight of federal cybersecurity R&D to increase the focus and efficiency of the programs. Currently several interagency groups focus on, or include cybersecurity research in their missions, but there is not a single group with primary responsibility. The committee recommends that the Interagency Working Group on Critical Information Infrastructure Protection become the focal point for coordinating Federal cyber security R&D efforts. One task for a strengthened version of this working group would be to systematically collect data on federal cybersecurity R&D efforts.

7. Witness Questions

The witnesses were asked to address the following questions in their testimony:

Questions for Dr. John Marburger:

- What are the Administration's highest priorities in computer science research? How and why have these priorities—and overall federal support for computer science research—changed in the last five years?
- What are the relative roles of the National Science Foundation and the Defense Advanced Research Projects Agency in supporting computer science research? How and why have these roles been changing?
- What is the Administration's response to the recent President's Information Technology Advisory Committee (PITAC) report on cybersecurity?

Questions for Dr. Anthony Tether :

- How does the Defense Advanced Research Projects Agency's (DARPA's) support for computer science research relate to its overall mission?
- What are DARPA's highest priorities in computer science research?
- How do you determine the balance between short- and long-term research programs? How does DARPA utilize academic and industrial researchers for computer science projects? Has the balance between short- and long-term research and between academic and industrial researchers within DARPA's computer science research portfolio changed in the last five years? If so, why?
- What is DARPA's response to the recent President's Information Technology Advisory Committee (PITAC) report on cybersecurity?

Questions for Dr. Wm. Wulf:

- What effects are shifts in federal support for computer science—e.g. shifts in the balance between short- and long-term research, shifts in the roles of different agencies—having on academic and industrial computer science research? What effects are changes in that research likely to have on the future of the U.S. information technology industry and on innovation in this field?
- Are the federal government's current priorities related to computer science research appropriate? If not, how should they be changed?
- What are your views on the recent President's Information Technology Advisory Committee (PITAC) report on cybersecurity? What should the federal government be doing to implement the recommendations of this report? Should PITAC be renewed when its current term expires on June 1?

Questions for Dr. Tom Leighton:

- Please explain the findings and recommendations of the recent President's Information Technology Advisory Committee (PITAC) report on *Cyber Security: A Crisis of Prioritization*.
- What role does cybersecurity research conducted at universities play in the development of cybersecurity tools and the implementation of good cybersecurity practices by U.S. companies?
- How have the composition and activities of the cybersecurity research community changed in recent years? How has federal support for cybersecurity research changed in recent years?

Attachment A

PENTAGON REDIRECTS ITS RESEARCH DOLLARS
New York Times, April 2, 2005, page C1
By John Markoff

SAN FRANCISCO, April 1 - The Defense Advanced Research Projects Agency at the Pentagon - which has long underwritten open-ended “blue sky” research by the nation’s best computer scientists - is sharply cutting such spending at universities, researchers say, in favor of financing more classified work and narrowly defined projects that promise a more immediate payoff.

Hundreds of research projects supported by the agency, known as Darpa, have paid off handsomely in recent decades, leading not only to new weapons, but to commercial technologies from the personal computer to the Internet. The agency has devoted hundreds of millions of dollars to basic software research, too, including work that led to such recent advances as the Web search technologies that Google and others have introduced.

The shift away from basic research is alarming many leading computer scientists and electrical engineers, who warn that there will be long-term consequences for the nation's economy. They are accusing the Pentagon of reining in an agency that has played a crucial role in fostering America’s lead in computer and communications technologies.

“I'm worried and depressed,” said David Patterson, a computer scientist at the University of California, Berkeley who is president of the Association of Computing Machinery, an industry and academic trade group. “I think there will be great technologies that won’t be there down the road when we need them.”

University researchers, usually reluctant to speak out, have started quietly challenging the agency’s new approach. They assert that Darpa has shifted a lot more work in recent years to military contractors, adopted a focus on short-term projects while cutting support for basic research, classified formerly open projects as secret and placed new restrictions on sharing information.

This week, in responding to a query from the staff of the Senate Armed Services Committee, Darpa officials acknowledged for the first time a shift in focus. They revealed that within a relatively steady budget for computer science research that rose slightly from $546 million in 2001 to $583 million last year, the portion going to university researchers has fallen from $214 million to $123 million.

The agency cited a number of reasons for the decline: increased reliance on corporate research; a need for more classified projects since 9/11; Congress’s decision to end controversial projects like Total Information Awareness because of privacy fears; and the shift of some basic research to advanced weapons systems development.

In Silicon Valley, executives are also starting to worry about the consequences of Darpa’s stinting on basic research in computer science.

“This has been a phenomenal system for harnessing intellectual horsepower for the country,” said David L. Tennenhouse, a former Darpa official who is now director of research for Intel. “We should be careful how we tinker with it.”

University scientists assert that the changes go even further than what Darpa has disclosed. As financing has dipped, the remaining research grants come with yet more restrictions, they say, often tightly linked to specific “deliverables” that discourage exploration and serendipitous discoveries.

Many grants also limit the use of graduate students to those who hold American citizenship, a rule that hits hard in computer science, where many researchers are foreign.

The shift at Darpa has been noted not just by those researchers directly involved in computing technologies, but by those in other fields supported by the agency.

“I can see they are after deliverables, but the unfortunate thing is that basic research gets squeezed out in the process,” said Wolfgang Porod, director of the Center for Nano Science

and Technology at the University of Notre Dame.

The concerns are highlighted in a report on the state of the nation's cybersecurity that was released with little fanfare in March by the President's Information Technology Advisory Committee. Darpa has long focused on long-term basic research projects with time horizons that exceed five years, the report notes, but by last year, very little of Darpa's financing was being directed toward fundamental research in the field.

"Virtually every aspect of information technology upon which we rely today bears the stamp of federally sponsored university research," said Ed Lazowska, a computer scientist at the University of Washington and co-chairman of the advisory panel. "The federal government is walking away from this role, killing the goose that laid the golden egg."

As a result of the new restrictions, a number of computer scientists said they had chosen not to work with Darpa any longer. Last year, the agency offered to support research by Leonard Kleinrock, a computer scientist at the University of California, Los Angeles who was one of the small group of researchers who developed the Arpanet, the 1960's predecessor to today's Internet.

Dr. Kleinrock said that he decided that he was not interested in the project when he learned that the agency was insisting that he employ only graduate assistants with American citizenship.

Darpa officials, who declined repeated requests for interviews, disputed the university researchers. The agency, which responded only in writing to questions, contended that the criticisms leveled by the advisory committee and other researchers were not accurate and that it had always supported a mix of longer- and shorter-term research.

"The key is a focus on high-risk, high-payoff research," Jan Walker, a Darpa spokeswoman, stated in an e-mail message. Given the threat from terrorism and the demands on troops in Iraq, she wrote, Darpa is rightly devoting more attention to "quick reaction" projects that draw on the fruits of earlier science and technology to produce useful prototypes as soon as possible.

The Pentagon shift has put added pressure on the other federal agencies that support basic information technology research.

At the Directorate for Computer and Information Science and Engineering of the National Science Foundation, the number of research proposals has soared from 2,000 in 1999 to 6,500 last year. Peter A. Freeman, its director, said that the sharp rise was partly attributable to declines in Pentagon support.

"Darpa has moved away from direct funding to universities," Mr. Freeman said. "Even when they do directly fund, some of the conditions and constraints seem to be pretty onerous. There is no question that the community doesn't like what the head of Darpa has been doing, but he has his reasons and his prerogatives."

The transformation of Darpa has been led by Anthony J. Tether, a Stanford-educated electrical engineer who has had a long career moving between executive positions at military contractors and the Pentagon.

Last year, Dr. Tether's new approach led to a series of cutbacks at a number of computer science departments. Program financing for a Darpa project known as Network Embedded Sensor Technology - intended to develop networks of sensors that could potentially be deployed on battlefields to locate and track enemy tanks and soldiers - has been cut back or ended on as many as five university campuses and shifted instead to traditional military contractors.

"The network has now become as vital as the weapons themselves," Dr. Tether said in an appearance before the advisory committee last year, testifying that secrecy had become more essential for a significant part of the agency's work.

That has created problems for university researchers. Several scientists have been instructed, for example, to remove previously published results from Web sites. And at U.C.L.A. and Berkeley, Darpa officials tried to classify software research done under a contract that specified that the results would be distributed under so-called open-source licensing terms.

"We were requested to remove all publicly accessible pointers to software

developed under the program," said Deborah Estrin, director of embedded network sensing at U.C.L.A. "This is the first time in 15 years that I have no Darpa funding."

At Berkeley, Edward A. Lee, who was recently named chairman of the computer science department, agreed not to publish a final report at Darpa's request, even though he told officials the data had already become widely available.

Despite the complaints, some pioneering researchers support the changes being driven by Dr. Tether and say they are necessary to prepare the nation for a long battle against elusive enemies.

"There are pressures and demands on Darpa to be relevant," said Robert Kahn, a former Darpa administrator who is now president of the Corporation for National Research Initiatives in Reston, Va. "People think it should stay the same, but times have changed."

Still, a number of top scientists argue that the Pentagon's shift in priorities could not have come at a worse time. Most American companies have largely ended basic research and have begun to outsource product research and development extensively even as investments in Asia and Europe are rising quickly.

And many computer scientists dispute Darpa's reasoning that fighting wars demands a shift away from basic research. During the Vietnam War, they say, Darpa kept its commitment to open-ended computer research, supporting things like a laboratory in the hills behind Stanford University dedicated to the far-out idea of building computing machines to mimic human capabilities.

John McCarthy founded the Stanford artificial research lab in 1964, helping to turn it into a wellspring for some of Silicon Valley's most important companies, from Xerox Parc to Apple to Intel.

"American leadership in computer science and in applications has benefited more from the longer-term work," Mr. McCarthy said, "than from the deliverables."

Attachment B

EDITORIAL: AN ENDLESS FRONTIER POSTPONED
SCIENCE Magazine, Volume 308, May 6, 2005, page 757
By Edward D. Lazowska and David A. Patterson

Next month, U.S. scientists Vinton G. Cerf and Robert E. Kahn will receive computing's highest prize, the A. M. Turing Award, from the Association for Computing Machinery. Their Transmission Control Protocol (TCP), created in 1973, became the language of the Internet. Twenty years later, the Mosaic Web browser gave the Internet its public face. TCP and Mosaic illustrate the nature of computer science research, combining a quest for fundamental understanding with considerations of use. They also illustrate the essential role of government-sponsored university-based research in producing the ideas and people that drive innovation in information technology (IT).

Recent changes in the U.S. funding landscape have put this innovation pipeline at risk. The Defense Advanced Research Projects Agency (DARPA) funded TCP. The shock of the Soviet satellite Sputnik in 1957 led to the creation of the agency, which was charged with preventing future technological surprises. From its inception, DARPA funded long-term nonclassified IT research in academia, even during several wars, to leverage all the best minds. Much of this research was dual-use, with the results ultimately advancing military systems and spurring the IT industry.

U.S. IT research grew largely under DARPA and the National Science Foundation (NSF). NSF relied on peer review, whereas DARPA bet on vision and reputation, complementary approaches that served the nation well. Over the past 4 decades, the resulting research has laid the foundation for the modern microprocessor, the Internet, the graphical user interface, and single-user workstations. It has also launched new fields such as computational science. Virtually every aspect of IT that we rely on today bears the stamp of federally sponsored research. A 2003 National Academies study provided 19 examples where such work ultimately led to billion-dollar industries, an economic benefit that reaffirms science advisor Vannevar Bush's 1945 vision in Science: The Endless Frontier.

However, in the past 3 years, DARPA funding for IT research at universities has dropped by nearly half. Policy changes at the agency, including increased classification of research programs, increased restrictions on the participation of noncitizens, and "go/no-go" reviews applied to research at 12- to 18-month intervals, discourage participation by university researchers and signal a shift from pushing the leading edge to "bridging the gap" between fundamental research and deployable technologies. In essence, NSF is now relied on to support the long-term research needed to advance the IT field.

Other agencies have not stepped in. The Defense Science Board noted in a recent look at microchip research at the Department of Defense (DOD): "[DARPA's] withdrawal has created a vacuum . . . The problem, for DOD, the IT industry, and the nation as a whole, is that no effective leadership structure has been substituted." The Department of Homeland Security, according to a recent report from the President's Information Technology Advisory Committee, spends less than 2% of its Science and Technology budget on cybersecurity, and only a small fraction of that on research. NASA is downsizing computational science, and IT research budgets at the Department of Energy and the National Institutes of Health are slated for cuts in the president's fiscal year 2006 budget.

These changes, combined with the growth of the discipline, have placed a significant burden on NSF, which is now showing the strain. Last year, NSF supported 86% of federal obligations for fundamental research in IT at academic institutions. The funding rate for competitive awards in the IT sector fell to 16%, the lowest of any directorate. Such low success rates are harmful to the discipline and, ultimately, to the nation.*

At a time when global competitors are gaining the capacity and commitment to challenge U.S. high-tech leadership, this changed landscape threatens to derail the extraordinarily productive interplay of academia, government, and industry in IT. Given the importance of IT in enabling the new economy and in opening new areas of scientific discovery, we simply cannot afford to cede leadership. Where will the next generation of groundbreaking innovations in IT arise? Where will the Turing Awardees 30 years hence reside? Given current trends, the answers to both questions will likely be, "not in the United States."

About the Authors: Edward D. Lazowska holds the Bill & Melinda Gates Chair in Computer Science & Engineering at the University of Washington. David A. Patterson holds the E. H. and M. E. Pardee Chair of Computer Science at the University of California, Berkeley, and is president of the Association for Computing Machinery. Both are members of the National Academy of Engineering and the President's Information Technology Advisory Committee, and past chairs of the Computing Research Association.

*The House Science Committee will consider these issues at a 12 May hearing on "The Future of Computer Science Research in the U.S." See http://www.cra.org/research.

Attachment C

CYBERSECURITY: A CRISIS OF PRIORITIZATION

Report to the President from the President's Information Technology Advisory Committee
Released March 2005

EXECUTIVE SUMMARY

The information technology (IT) infrastructure of the United States, which is now vital for communication, commerce, and control of our physical infrastructure, is highly vulnerable to terrorist and criminal attacks. The private sector has an important role in securing the Nation's IT infrastructure by deploying sound security products and adopting good security practices. But the Federal government also has a key role to play by supporting the discovery and development of cyber security technologies that underpin these products and practices. The PITAC finds that the Federal government needs to fundamentally improve its approach to cyber security to fulfill its responsibilities in this regard.

Background

The Nation's IT infrastructure has undergone a dramatic transformation over the last decade. Explosive growth in the use of networks to connect various IT systems has made it relatively easy to obtain information, to communicate, and to control these systems across great distances. Because of the tremendous productivity gains and new capabilities enabled by these networked systems, they have been incorporated into a vast number of civilian applications, including education, commerce, science and engineering, and entertainment. They have also been incorporated into virtually every sector of the Nation's critical infrastructure – including communications, utilities, finance, transportation, law enforcement, and defense. Indeed, these sectors are now critically reliant on the underlying IT infrastructure.

At the same time, this revolution in connectivity has also increased the potential of those who would do harm, giving them the capability to do so from afar while armed with only a computer and the knowledge needed to identify and exploit vulnerabilities. Today, it is possible for a malicious agent to penetrate millions of computers around the world in a matter of minutes, exploiting those machines to attack the Nation's critical infrastructure, penetrate sensitive systems, or steal valuable data. The growth in the number of attacks matches the tremendous growth in connectivity, and dealing with these attacks now costs the Nation billions of dollars annually. Moreover, we are rapidly losing ground to those who do harm, as is indicated by the steadily mounting numbers of compromised networks and resulting financial losses.

Beyond economic repercussions, the risks to our Nation's security are clear. In addition to the potential for attacks on critical targets within our borders, our national defense systems are at risk as well, because the military increasingly relies on ubiquitous communication and the networks that support it. The Global Information Grid (GIG), which is projected to cost as much as $100 billion and is intended to improve military communications by linking weapons, intelligence, and military personnel to each other, represents one such critical network. Since military networks interconnect with those in the civilian sector or use similar hardware or software, they are susceptible to any vulnerability in these other networks or technologies. Thus cyber security in the civilian and military sectors is intrinsically linked.

Although the large costs associated with cyber insecurity have only recently become manifest, the Nation's cyber security problems have been building for many years and will plague us for many years to come. They derive from a decades-long failure to develop the security protocols and practices needed to protect the Nation's IT infrastructure, and to adequately train and grow the numbers of experts needed to employ those mechanisms effectively. The short-term patches and fixes that are deployed today can be useful in response to isolated vulnerabilities, but they do not adequately address the core problems. Rather, fundamental, long-term research is required to develop entirely new approaches to cyber security. It is imperative that we take action before the situation worsens and the cost of inaction becomes even greater.

Summary of Findings and Recommendations

The PITAC's recommendations on cyber security, and the findings upon which those recommendations are based, are summarized below.

Issue 1: Federal Funding Levels for Fundamental Research in Civilian Cyber Security

Long-term, fundamental research in cyber security requires a significant investment by the Federal government because market forces direct private sector investment away from research and toward the application of existing technologies to develop marketable products. However, Federal funding for cyber security research has shifted from long-term, fundamental research toward shorter-term research and development, and from civilian research toward military and intelligence applications. Research in these domains is often classified and the results are thus unavailable for use in securing civilian IT infrastructure and commercial off-the-shelf (COTS) products in widespread use by both government and the civilian sector. These changes have been particularly dramatic at the Defense Advanced Research Projects Agency (DARPA) and the National Security Agency (NSA); other agencies, such as the National Science Foundation (NSF) and the Department of Homeland Security (DHS), have not stepped in to fill the gaps that have been created. As a result, investment in fundamental research in civilian cyber security is decreasing at the time when it is most desperately needed.

The PITAC finds that the Federal R&D budget provides inadequate funding for fundamental research in civilian cyber security, and recommends that the NSF budget in this area be increased by $90 million annually. Funding for fundamental research in civilian cyber security should also be substantially increased at other agencies, most notably DHS and DARPA. Funding should be allocated so that at least the ten specific areas listed in the "Cyber Security Research Priorities" section beginning on page 37 of Chapter 4 are appropriately addressed. Further increases in funding may be necessary depending on the Nation's future cyber security posture.

Issue 2: The Cyber Security Fundamental Research Community

Improving the Nation's cyber security posture requires highly trained people to develop, deploy, and incorporate new cyber security products and practices. The number of such highly trained people in the U.S. is too small given the magnitude of the challenge. At U.S. academic institutions today, the PITAC estimates, there are fewer than 250 active cyber security or cyber assurance specialists, many of whom lack either formal training or extensive professional experience in the field. In part, this situation exists because cyber security has historically been the focus of a small segment of the computer science and engineering research community. The

situation has been exacerbated by the insufficient and unstable funding levels for long-term, civilian cyber security research, which universities depend upon to attract and retain faculty.

The PITAC finds that the Nation's cyber security research community is too small to adequately support the cyber security research and education programs necessary to protect the United States. The PITAC recommends that the Federal government intensify its efforts to promote recruitment and retention of cyber security researchers and students at research universities, with a goal of at least doubling the size of the civilian cyber security fundamental research community by the end of the decade. In particular, the Federal government should increase and stabilize funding for fundamental research in civilian cyber security, and should support programs that enable researchers to move into cyber security research from other fields.

Issue 3: Translating Research into Effective Cyber Security for the Nation

Technology transfer enables the results of Federally supported R&D to be incorporated into products that are available for general use. There has been a long and successful history of Federally funded IT R&D being transferred into products and best practices that are widely adopted in the private sector, in many cases spawning entirely new billion-dollar industries. Technology transfer has been particularly challenging in the area of cyber security, however, because the value of a good cyber security product to the consumer lies in the reduced incidence of successful attacks – a factor difficult to quantify in the short term as a return on investment.

The PITAC finds that current cyber security technology transfer efforts are not adequate to successfully transition Federal research investments into civilian sector best practices and products. As a result, the PITAC recommends that the Federal government strengthen its cyber security technology transfer partnership with the private sector. Specifically, the Federal government should place greater emphasis on the development of metrics, models, datasets, and testbeds so that new products and best practices can be evaluated; jointly sponsor with the private sector an annual interagency conference at which new cyber security R&D results are showcased; fund technology transfer efforts (in cooperation with industry) by researchers who have developed promising ideas or technologies; and encourage Federally supported graduate students and postdoctoral researchers to gain experience in industry as researchers, interns, or consultants.

Issue 4: Coordination and Oversight for Federal Cyber Security R&D

One of the key problems with the Federal government's current approach to cyber security is that the government-wide coordination of cyber security R&D is ineffective. Research agendas and programs are not systematically coordinated across agencies and, as a result, misconceptions among agencies regarding each others' programs and responsibilities have been allowed to develop, causing important priorities to be overlooked. In the absence of coordination, individual agencies focus on their individual missions and can lose sight of overarching national needs. Initiatives to strengthen and enlarge the cyber security research community and efforts to implement the results of R&D would be more effective and efficient with significantly stronger coordination across the Federal government.

The PITAC finds that the overall Federal cyber security R&D effort is currently unfocused and inefficient because of inadequate coordination and oversight. To remedy this situation, PITAC recommends that the Interagency Working Group on Critical Information Infrastructure Protection (CIIP) become the focal point for coordinating Federal cyber security

R&D efforts. This working group should be strengthened and integrated under the Networking and Information Technology Research and Development (NITRD) Program.